# Sécurité : Telegram, une vulnérabilité qui prête à discussion

Une grave affaire prise à la légère ou, au contraire, beaucoup de bruit pour rien ? Les avis sont partagés à propos de la faille de sécurité découverte sur **Telegram** par le dénommé Kirill Firsov.

Ce chercheur russe s'est aperçu que la version Mac du service sécurisé de messagerie enregistrait, dans les journaux système (*syslog*), chaque message collé dans le champ de discussion depuis le presse-papiers. Le 23 juillet, il avait, sur Twitter, interpellé Pavel Durov, cofondateur du service avec son frère Nikolai.

S'est ensuivi un échange de tweets à l'issue duquel le bug a été résolu… sans qu'on puisse mesurer quelle était sa réelle ampleur. L'explication entre les deux hommes s'est effectivement terminée sur un « Imagine que la police saisisse ton ordinateur portable et qu'elle retrouve trace de tes messages 'secrets' dans syslog » lancé par Kirill Firsov.

## La sandbox pour limiter les dégâts

Pour Pavel Durov, la vulnérabilité, repérée sur les versions 2.16 et 2.17 de Telegram, n'est pas aussi importante qu'elle en a l'air : n'est concerné que le texte collé depuis le presse-papiers… auquel toutes les autres applications Mac ont accès.

Sans nier cet état de fait, Kirill Firsov avait pointé du doigt le fait que les messages font l'objet d'une journalisation. Ce à quoi Pavel Durov avait répondu qu'avec le mécanisme dit de « bac à sable » (*sandbox*), les applications téléchargées sur l'App Store d'OS X – à l'image de Telegram – ne peuvent qu'écrire dans *syslog* ; pas y accéder en lecture (voir, à ce propos, la documentation d'Apple).

Bilan pour celui qui a financé Telegram via son fonds Digital Fortress, corriger la faille revient juste à éliminer une redondance : le fait que toutes les applications peuvent accéder au contenu du presse-papiers.

## Le service qui monte

L'histoire de Telegram est particulière. Ses fondateurs s'étaient installés à Berlin après avoir, sur fond de lutte d'influence politique avec l'entourage de Vladimir Poutine, perdu le contrôle du réseau social vKontakte, qu'ils avaient créé en Russie.

Utilisé à l'origine par les seules équipes de vKontakte, Telegram avait basculé, en 2013, dans une exploitation ouverte au grand public.

En insistant sur la dimension de confidentialité des échanges, le service a dépassé, fin février, les 100 millions d'utilisateurs actifs par mois, souligne ITespresso.

Une ascension qui n'a pas laissé la concurrence indifférente. Illustration chez WhatsApp, qui avait décidé, fin 2015, de bloquer, sur Android, les liens vers l'application Telegram diffusés par ses

utilisateurs.

Le service, qui exploite un protocole de chiffrement maison (MTProto), a aussi été mis en lumière pour des considérations plus sombres : selon Trend Micro, 34 % des organisations terroristes l'utilisent comme point de contact.

**A lire aussi :**

Après les attentats, la messagerie chiffrée Telegram met (un peu) d'ordre

La Russie prête à fragiliser le chiffrement de messageries ?

**Denys Prykhodov / Shutterstock**